AO 91 (Rev. 02/09) Criminal Complaint

United States District Court

for the
Western District of New York

United States of America

v.

Case No. 23-MJ-5097

COREY ROBERT DODGE, a/k/a Cakesbaylor

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about April 2, 2020, the exact date being unknown, in the Western District of New York, and elsewhere, the defendant, COREY ROBERT DODGE, a/k/a Cakesbaylor, knowingly and with intent to defraud, possessed fifteen or more unauthorized access devices, as defined in Title 18, United States Code, Section 1029(e)(3), that is, stolen login credentials, said possession affecting interstate and foreign commerce in that the defendant purchased the unauthorized access devices from a website based outside the United States.

All in violation of Title 18, United States Code, Section 1029(a)(3).

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

Complainant's signature

BRYAN SCHEIBER
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION
Printed name and title

Sworn to before me and signed telephonically.

Date: April 27, 2023

Judge's signature

City and State: Buffalo, New York

HONORABLE MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Bryan Scheiber, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a criminal complaint charging **COREY ROBERT DODGE** (hereinafter "DODGE"), with a violation of Title 18, United States Code, Section 1029(a)(3) (knowingly and with intent to defraud possessing fifteen or more devices which are counterfeit or unauthorized access devices).

2. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since June 2021. I am currently assigned to the FBI Buffalo Field Office Cyber Task Force in Buffalo, New York, where I work on investigations relating to criminal and national security cyber intrusions. I received my Bachelor's and Master's degrees in Computer Science, have a Graduate Certificate in Computer Security and Information Assurance and hold several private sector computer security certifications. Prior to becoming an FBI Special Agent, I was a Computer Scientist with the FBI's Washington Field Office. My work in the FBI, as well as the training I have received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against the United States.

3. The facts set forth are based upon my personal observations, my training and experience, and information obtained during the course of the investigation from other members of law enforcement, involving the review of records, interviews of subjects and witnesses, and information and reports provided. Because this affidavit is submitted for the purpose of

establishing probable cause to support the issuance of a Criminal Complaint and Arrest Warrant, I have not included each and every fact known by the government for this investigation.

4. The facts set forth are based upon my personal observations, my training and experience, and information obtained during the course of the investigation from other members of law enforcement, involving the review of records, interviews of witnesses, and information and reports provided. Because this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a Criminal Complaint and Arrest Warrant, I have not included each and every fact known by the government for this investigation.

PROBABLE CAUSE

Background Regarding the Genesis Market Investigation

5. Since August 2018, the FBI has been investigating an illicit online marketplace named Genesis Market.[1] Genesis Market is primarily hosted at the Internet domain "genesis.market."[2] Genesis Market's operators compile stolen data (*e.g.*, computer and mobile

---

[1] In Attachment B, Genesis Market is referred to "Web Market A." At this time, Genesis Market remains active and disclosure of the name of the market would potentially alert its operators of law enforcement action being taken against the users and operators. This may prompt users of the market to notify others of law enforcement action, flee, and/or destroy evidence. Accordingly, the government will file a separate motion to seal the warrant affidavit.

[2] A domain name is a way to identify computers on the Internet, using a series of characters that correspond with a particular IP address. Genesis Market is also associated with certain backup domains in case the primary domain is shut down or taken offline for any reason. Those backup domains include the website "g3n3sis.org," as well as the TOR domain "genesiswiwn7p7lmbvimup7v767e64rcw6o3kfcnobu3nxisteprx2qd.onion." TOR is short for "The Onion Router" and is free, publicly available software for enabling anonymous communication over the internet. The TOR software is designed to enhance users' privacy online by bouncing their communications around a

device identifiers, email addresses, usernames, and passwords) from malware-infected[3] computers around the globe and package it for sale on the market.[4] Genesis Market has been the subject of various cybersecurity presentations and news stories. For example, CBS News ran a story on Genesis Market in September 2021.[5]

6. The packages advertised for sale on Genesis Market vary by price and many packages are available for around $10 to $20 per package. The price appears to vary based on three primary factors: (1) the number of online accounts ("resources") associated with the package (*e.g.*, accounts with legitimate credentials for platforms like Amazon, Netflix, Gmail, etc. are more valuable); (2) how recently the package was compromised with malware; and (3) whether there is a "fingerprint" associated with the package. A fingerprint is a group of identifiers that third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. In

---

distributed network of relay computers run by volunteers around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user.

[3] Malware, or malicious software, refers to any piece of software that is written to damage and/or steal data from an Internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

[4] Genesis Market refers to these packages of stolen data as "bots" on their site; however, typically, an Internet bot refers to a piece of software that runs automated tasks over the Internet. Since Genesis Market's use of the word "bot" strays from the normal meaning, the term "package" is used throughout this request.

[5] See Dan Patterson, *Inside Genesis: The market created by cybercriminals to make millions selling your digital identity*, September 9, 2021, available at https://www.cbsnews.com/news/genesis-cybercriminal-market-ransomware/ (last visited March 13, 2023).

situations where a fingerprint is associated with a package, Genesis Market provides the purchaser with a proprietary plugin (*i.e.*, an Internet browser extension that provides additional functionality). This proprietary plugin amplifies that purchaser's ability to control and access the package's data and masquerade as the victim device.

7. Genesis Market's operators have advertised Genesis Market on prominent online criminal forums, including exploit.in and xss.is. Those advertisements include news, updates, and information regarding Genesis Market. For example, the advertisements have included (1) information about packages for sale on Genesis Market; (2) specific replies to users requesting packages located in specific countries; and (3) updates regarding the tools available through Genesis Market.

8. Genesis Market users can gain initial access to Genesis Market via an invitation from a Genesis Market operator on a cybercriminal forum, or via an invitation from an individual who already has an account on Genesis Market. The invitations are for one-time use and in the form of an alphanumeric text string. Once a prospective new user receives an invitation, the new user can go to a Genesis Market domain to create a username and password. Genesis Market then requests the new user to associate their Jabber ID[6] or email address with that new account. Analysis by law enforcement has found that a Jabber ID or email address is not absolutely

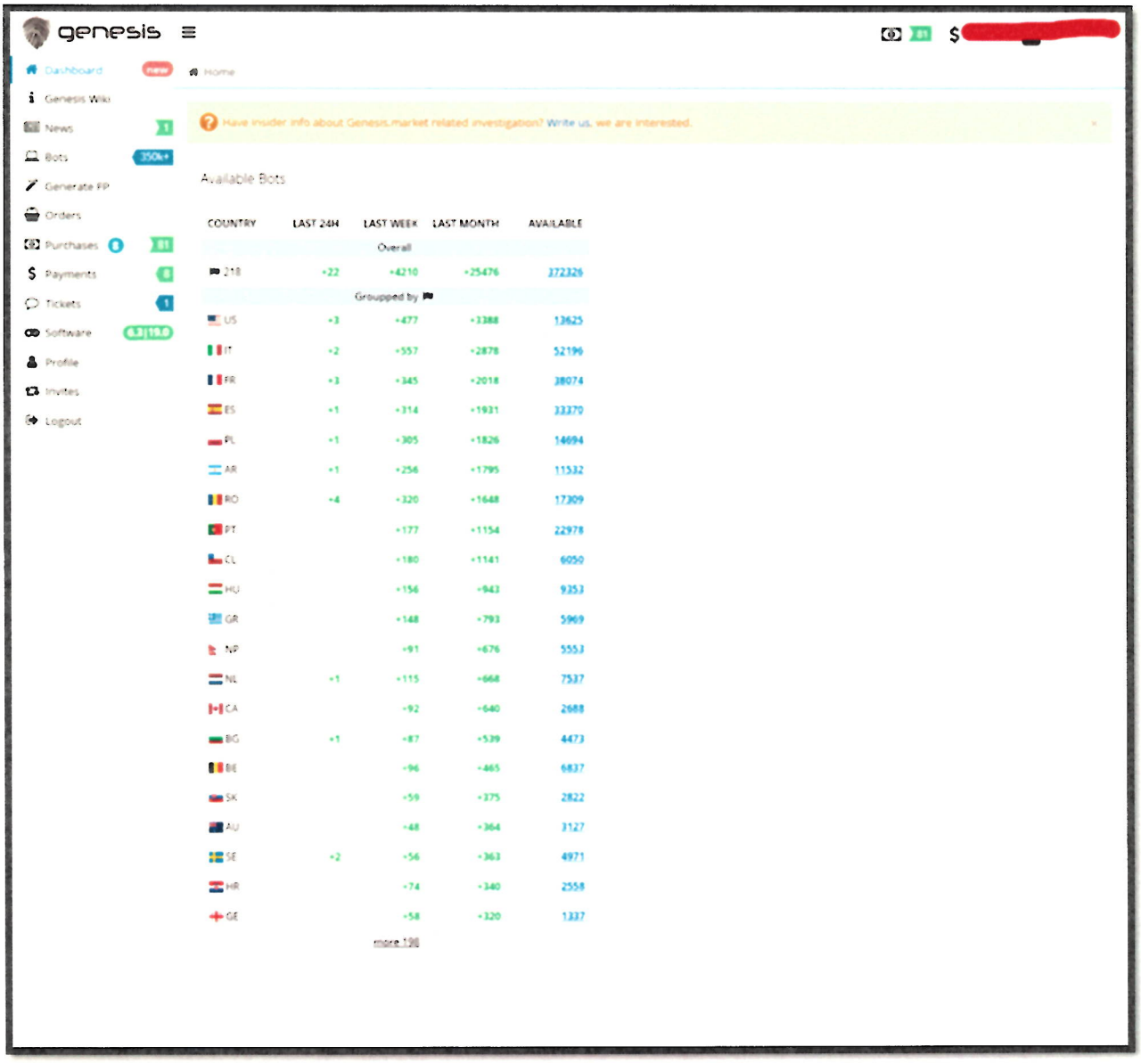
[6] Jabber is a chat and communications platform akin to AOL Instant Messenger. It is prominent among cybercriminal operators because it is considered exceptionally secure.

required when registering an account, nor is the Jabber ID or email address verified by Genesis Market administrators. Nonetheless, the vast majority of Genesis users have registered with a Jabber ID or email address, as it is one of the fields to enter registration data when creating a new account.

9. While conducting covert operations, law enforcement has observed that for new users logged into Genesis Market, the front page generally displays a "dashboard" of information, including the number of packages listed for sale and a "Genesis Wiki" page that walks a new user through Genesis Market's platform and how to use it. Below is a screenshot taken April 1, 2021, of the front page of Genesis Market.[7] The front page displays the total amount of "bots" (packages) available for sale on Genesis Market at that time, categorized by country. This page appears immediately after the user logs into his or her account. The tabs on the left allow for the Genesis Market user to traverse the market:

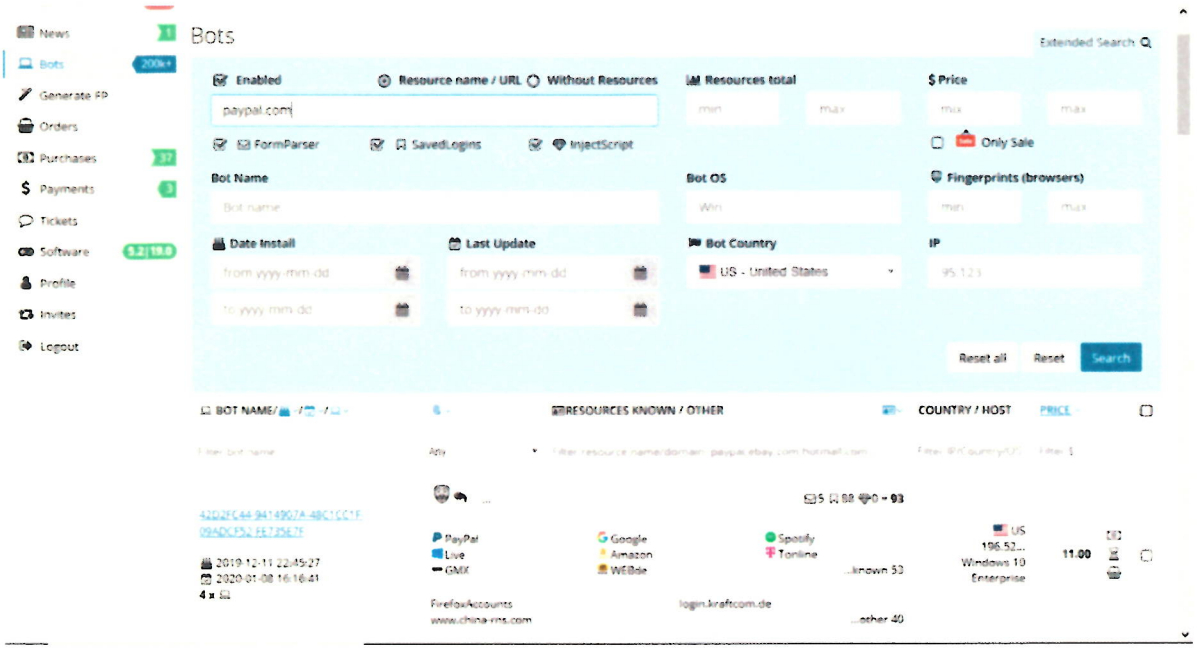
---

[7] Portions of the screenshots in this affidavit have been redacted or omitted to conceal information that might identify accounts used covertly by investigators.

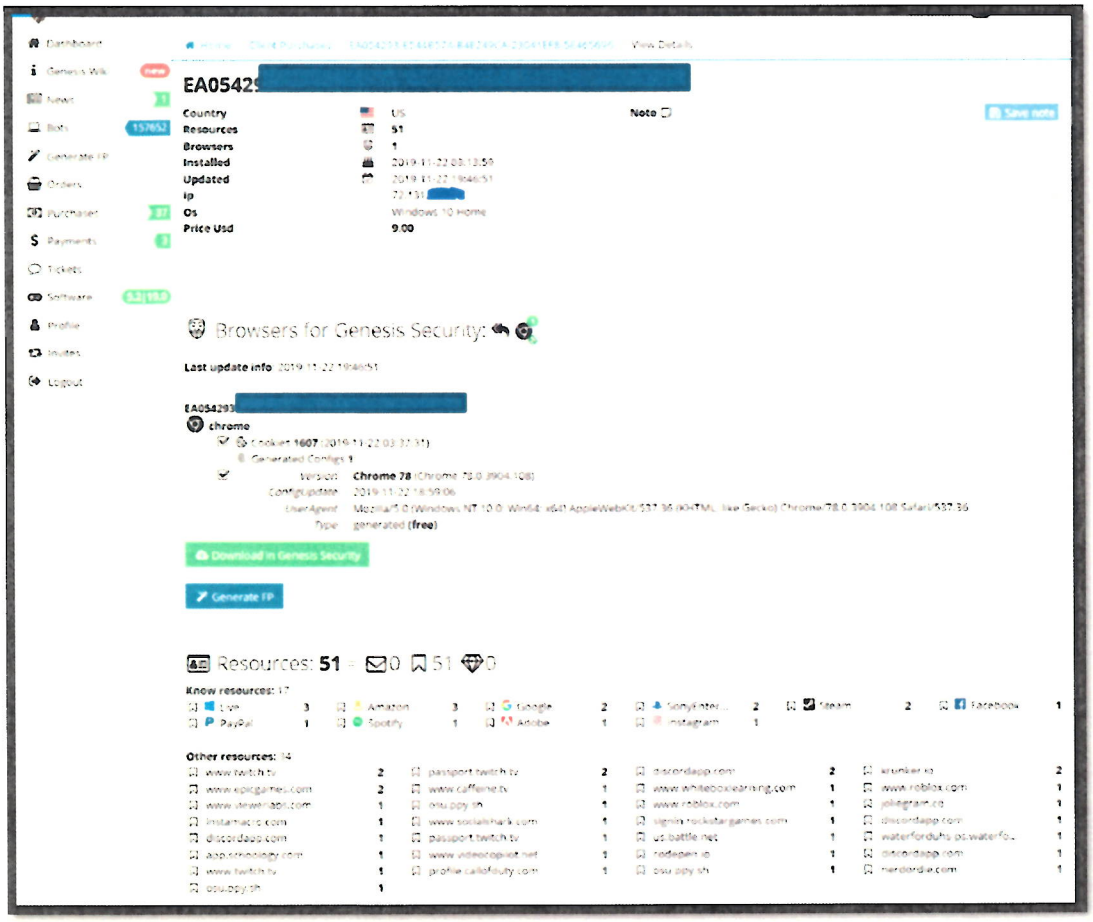


10. Genesis Market also features a search function that allows a user to search for packages based on areas of interest (*e.g.*, banking information, social media accounts, etc.),

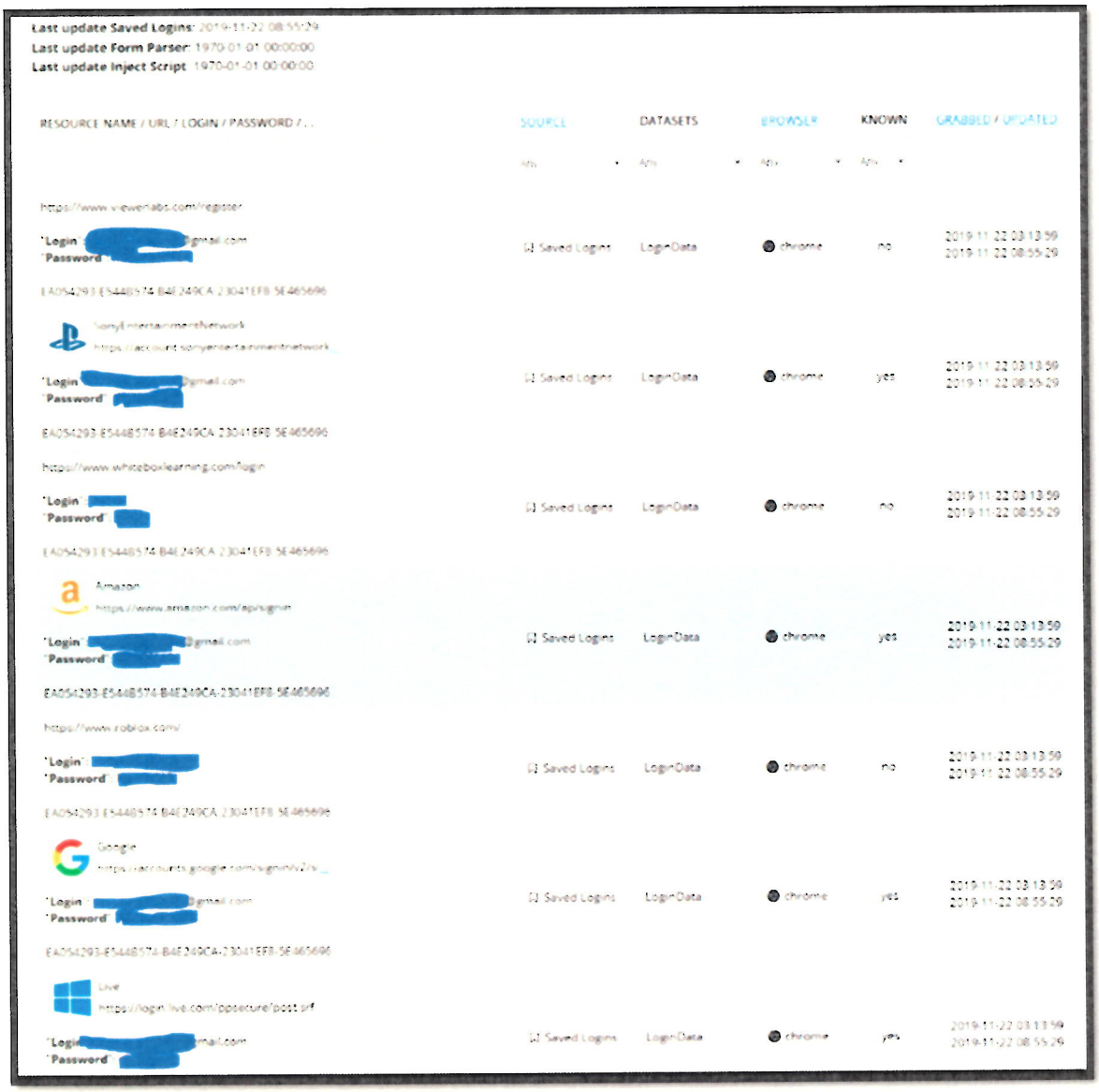
country of origin, price, and the date of infection (*i.e.*, the date the victim device was infected with malware). Below is a screenshot taken on November 13, 2020, showing the search function on Genesis Market:



11. When a user purchases a package, the user receives access to all the identifiers associated with the package, including, but not necessarily limited to, device information, such as operating system, IP address, keyboard language, and time zone information, as well as access credentials, such as usernames and passwords, for compromised accounts. Below is a screenshot taken on November 22, 2019, of an FBI Online Covert Employee's purchase of a Genesis Market package:



12. Below is a screenshot dated November 22, 2019, relating to the same victim package as above, showing the email addresses and passwords (both of which are redacted for the purposes of this affidavit) that are provided to the purchaser of the victim package:



13. When users have questions or issues with Genesis Market, they can submit "tickets" via a "Ticket" tab on the Genesis Market website, which enables them to communicate with Genesis Market operators.

14. Purchases made through Genesis Market are conducted using virtual currency, such as bitcoin.[8] Before a purchase can be made, however, the user must first deposit a sum of virtual currency into their Genesis Market account. This is done through the "Payments" tab on the Genesis Market website, wherein the user can choose the type of virtual currency they want to use. If the user chose bitcoin, for example, the user would then (1) enter the amount in U.S. dollars that they want credited to their account, (2) receive a one-time-use bitcoin address, along with the converted bitcoin amount, and then (3) they would use that bitcoin address to send bitcoin to Genesis Market.[9] Once the user sends the bitcoin to the one-time-use address, the user is prompted to wait several minutes for the transaction to complete, and then the user will ultimately see that their Genesis Market account is credited with the requested amount. Once the account is credited, the user can purchase packages from Genesis Market.

15. As of October 17, 2022, there were approximately 450,000 packages listed for sale on Genesis Market. Each package represents a single, compromised computer or device.

---

[8] Virtual currencies, such as bitcoin, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use. Investigators found that Genesis Market also accepted Litecoin (an alternative to bitcoin), and in 2022 started accepting Monero (an anonymity enhanced virtual currency).

[9] Over the course of the investigation, investigators found that Genesis Market utilized a third-party service, the identify of which is known to law enforcement and known to be associated with criminal activity, to process the virtual currency transactions.

According to Genesis Market's website, the packages are located across North America (including throughout the United States), Europe, South America, and parts of Asia.

16. As part of the investigation, the FBI has covertly operated several Genesis Market accounts and has funded the purchase of approximately 115 packages through Genesis Market. Through these accounts, the FBI has monitored activity on Genesis Market and interacted with Genesis Market operators through the "Ticket" function. The FBI has reviewed the data from purchased packages and determined that Genesis Market is, in fact, collecting and selling victims' personal identifying information that has been stolen from devices located around the world. For instance, FBI agents identified seven packages that consisted of data taken from devices of victims located in Wisconsin. FBI agents showed seven victim device owners the usernames and passwords that the agents had obtained via Genesis Market, and the victims confirmed that the usernames and passwords belonged to them and had been stolen.

17. In December 2020, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as "Database A"). The database included, among other things, Genesis Market's administrator logs; user logs; lists of all packages sold on the marketplace; payment transaction logs; malware used by Genesis Market administrators; and other pieces of information related to the market.

18. The data included information from more than 33,000 Genesis Market user accounts, including usernames and email addresses; IP address history; search history; virtual

currency transactions; the number of packages purchased by the user; and the data contained within the packages purchased by the user.

19. After law enforcement obtained a copy of the Genesis Market Database A server, the Genesis Market operators removed their website from that server and utilized hosting infrastructure from other companies in other countries.

20. Then, in May 2022, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as "Database B"). The database included the same types of information described above, including information from more than 55,000 Genesis Market user accounts.

CakesBaylor's Activity on Genesis Market

21. The Genesis Market data showed that, from March 26, 2020 to May 30, 2021, a user whose account name was CakesBaylor purchased 14 packages on Genesis Market, that included approximately 8,586 stolen account credentials. The registration data for CakesBaylor showed the account was created on March 26, 2020, listed a Jabber ID address of williambauer56@protonmail.com, and deposited $289.12 to the marketplace. CakesBaylor queried Genesis Market for packages that included accounts for Paypal, Tracfone, eBay, Amazon, FedEx, Etsy, Walmart, Chase, Robin HoodVenmo, eTrade and the terms "credit card", "liquidation", "bank", "USbank", "tradestation", "tdameritrade" and "phone".

22. The Genesis Market data showed that CakesBaylor purchased the following packages on the marketplace:[10]

a. PACKAGE 1, which included compromised credentials for a victim's Google, eBay, Twitch, Codecademy, Sony Entertainment Network, GMX, Cybrary, Steam, Green Dot, Paypal, Instagram, LinkedIn, Hulu, CollegeBoard, Netspend, Netflix and Facebook accounts.

b. PACKAGE 2, which included compromised credentials for a victim's Facebook, Discord, Paypal, Github, Instagram, Google, Twitch, Valencia College Atlas, Amazon, Netflix, Target.com, Spotify and Steam accounts.

c. PACKAGE 3, which included compromised credentials for a victim's Microsoft Live, Google, Khan Academy, eBay, Instagram, Minecraft, Facebook, PowerSchool, Dropbox, Amazon and Paypal accounts.

d. PACKAGE 4, which included compromised credentials for a victim's Google, Steam, Disney Plus, Epic Games, Facebook, Paypal, Dearborn Schools, Discord, Microsoft Live, NordVPN, Amazon, Apple and Hulu accounts.

---

[10] As noted, CakesBaylor purchased more than 8,000 stolen credentials. This summary is therefore not an exclusive list of the credentials that CakesBaylor purchased.

e. PACKAGE 5, which included compromised credentials for a victim's GMX, iCloud, Yahoo, Spotify, Prezi, Google, Discord, Adobe ID, Facebook, Ryan Air, AutoDesk and LinkedIn accounts.

f. PACKAGE 6, which included compromised credentials for a victim's Google, Instagram, Paypal, Coinbase, Spotify, Wells Fargo, Patreon, eBay, Dropbox, Adobe ID, Khan Academy, Apple ID, Yahoo, Granite School District, Twitter, Discord, and Comcast accounts.

g. PACKAGE 7, which included compromised credentials for a victim's Microsoft Live, Github, Paypal, Discord, SoundCloud and Google accounts.

h. PACKAGE 8, which included compromised credentials for a victim's Facebook, Glock Cash Card, FedEx, USPS, Amazon, Pandora, Twitter, Chrysler, Charter, Paypal, and Sony accounts.

i. PACKAGE 9, which included compromised credentials for a victim's Google, United Community Bank, IBC Bank Online, Green State Credit Union, Instagram, Sams Club, and Spotify accounts.

j. PACKAGE 10, which included compromised credentials for a victim's Discord, Twitter, Craigslist, TurboTax, PACER, Paypal and Facebook accounts.

k. PACKAGE 11, which included compromised credentials for a victim's ADP, Paypal, Twitch and Twitter accounts.

l. PACKAGE 12, which included compromised credentials for a victim's Google, Microsoft Live and Facebook accounts.

m. PACKAGE 13, which included compromised credentials for a victim's Facebook, Google, Yahoo, Steam and Twitter accounts.

n. PACKAGE 14, which included compromised credentials for a victim's Facebook, Blockchain, AutoDesk, Google, LinkedIn, Twitter and Zoom accounts.

23. CakesBaylor accessed Genesis Market from IP addresses that were associated with Virtual Private Network ("VPN") services[11], such as IPVanish VPN and Psiphon 3, and IP addresses that may have been associated with residential proxy services[12]. Residential proxy services are often marketed to people seeking the ability to evade country-specific blocking by media streaming providers, but based on my training and experience, are also abused by those engaging in cybercrime activity because their use will trace malicious traffic to an unsuspecting residence, rather than its original source. Residential proxy services are difficult to detect because they appear to be legitimate traffic. For example, the residential proxy service 911.re provided customers with access to over 120,000 residential computers that could be used to

---

[11] VPN services route the user's internet traffic through the VPN provider's server network, concealing the user's original IP address and geographic location from visited websites with IP addresses assigned to the VPN provider's server network.

[12] Residential proxy services route the user's traffic through residential Internet Service Provider ("ISP") IP addresses. From a website's perspective, the traffic from a residential proxy service appears to originate from a residence rather than a VPN provider's server network and may appear more legitimate to the website.

proxy their traffic through.[13] CakesBaylor accessed Genesis Market from IP addresses that geolocated to locations as Colorado, Michigan, Pakistan, Italy and Egypt. Based on my training and experience, IP activity like this is indicative of the use of either a VPN or a residential proxy service.

24. CakesBaylor funded their Genesis Market account through two bitcoin transactions: Transaction 1 on March 26, 2020 for 0.0131 bitcoin with the transaction hash 91bc2e77cacc0eb5ae01f58447dec4d8821831ef7d128100b739081761f3fb57, and Transaction 2 on April 3, 2020 for 0.02992 bitcoin with the transaction hash 870c3506ea5f3c6508e6c52d83e6335be98266c5917b9f687b894de2cb1d6544. Investigators conducted cryptocurrency tracing and found that Transaction 1 originated from a cryptocurrency exchange named Block, Inc. and Transaction 2 originated from a cryptocurrency exchange named Coinbase.

25. Subpoena returns from Block, Inc. for Transaction 1 showed the transaction was associated with a Block, Inc. account for DODGE with the account address listed as 498 W Ferry St, Buffalo, NY 14213 (the PREMISES) and the email address listed as coreyrocksallday@yahoo.com. Block, Inc. provided Know Your Customer ("KYC") documents

---

[13] See: *Illegitimate residential proxy services: the case of 911.re and its IOCs* by Marc Frappier, Philippe-Antoine Plante, Guillaume Joly available at https://gric.recherche.usherbrooke.ca/rpaas/ (last visited March 13, 2023)

for DODGE that included front and back photographs of DODGE's New York State Driver License, which listed the PREMISES as DODGE's residence.

26. Subpoena returns from Coinbase for Transaction 2 showed the transaction was associated with a Coinbase account for DODGE with the account address listed as 498 W. Ferry St., Buffalo, NY 14213 (the PREMISES) and email address listed as coreyrocksallday@yahoo.com. Coinbase provided KYC documents for DODGE that included photographs of DODGE's New York State Driver License, which listed the PREMISES as DODGE's residence, and DODGE's United States of America Passport Card. Coinbase's identity verification process may request the customer hold their identification document next to their face in front of a camera. In this case, Coinbase provided a KYC photograph that showed DODGE holding his United States Passport Card.

27. Coinbase's response to the subpoena for Transaction 2 included an event log for DODGE's Coinbase account. That event log showed Transaction 2 was sent from DODGE's Coinbase account on April 3, 2020 at 15:57, i.e., the same day that Genesis Market showed that Transaction 2 was funded. Immediately prior to the transaction, DODGE's Coinbase account had a second factor prompt over SMS to a telephone number, TELEPHONE 1, that was verified with a subsequent login on April 3, 2020 at 15:53. Open source Caller ID queries for TELEPHONE 1 returned "DODGE COREY". Coinbase's event log for DODGE's Coinbase account showed the device that conducted this transaction had access to the Coinbase account since at least December 19, 2019 based on the IP address and Coinbase's fingerprint.

28. On April 4, 2020, CakesBaylor searched Genesis Market for packages that included Paypal accounts and generated a fingerprint for Bot ID 363284 which included Paypal credentials for VICTIM EMAIL 1. CakesBaylor accessed Genesis Market from the IP address 75.70.241.53 on April 4, 2020 at approximately 8:13 (timezone unknown).

29. Subpoena returns from Paypal for the Paypal account associated with VICTIM EMAIL 1 found that on April 4, 2020 at approximately 1:53 PST/PDT, the IP address 75.70.241.53 attempted to login to the Paypal account associated with VICTIM EMAIL 1 but was prompted with an SMS authentication challenge that did not appear to be successful.

30. IP address 75.70.241.53 was registered to Comcast Cable Communications Inc. and geolocated to Colorado Springs, Colorado. The investigation found that VICTIM EMAIL 1 was associated with an individual who resided in Colorado Springs, Colorado.

31. On April 8, 2020, CakesBaylor searched Genesis Market for packages that included Paypal accounts and generated a fingerprint for Bot ID 838673 which included Paypal credentials for VICTIM EMAIL 2. CakesBaylor accessed Genesis Market from the IP address 73.145.104.211 on April 8, 2020 at 7:19 (timezone unknown).

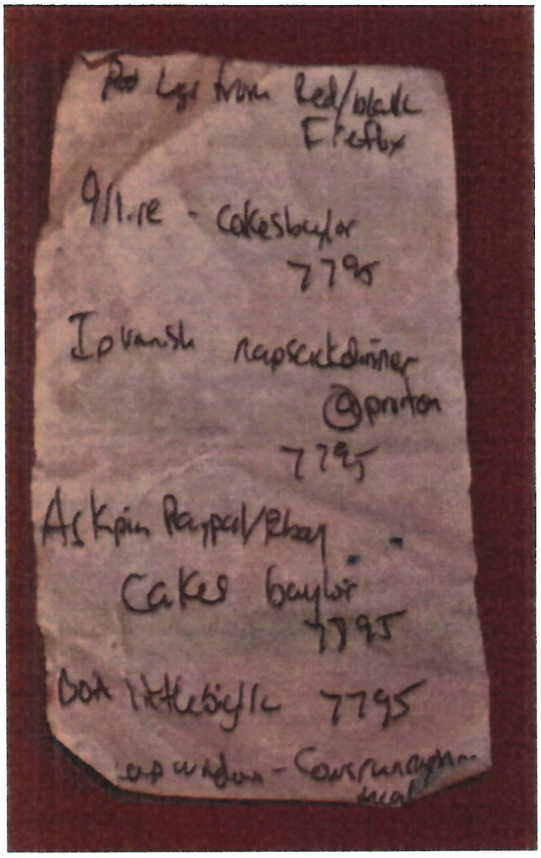
32. Subpoena returns from Paypal for the Paypal account associated with VICTIM EMAIL 2 found that on April 8, 2020 at 1:32 PST/PDT, the IP address 73.145.104.211 attempted to login to the Paypal account associated with VICTIM EMAIL 2 multiple times but did not appear to be successful.

33. IP address 73.145.104.211 was registered to Comcast Cable Communications Inc. and geolocated to Detroit, Michigan. Investigation found VICTIM EMAIL 2 was associated with an individual who resided in Dearborn, Michigan. Dearborn is a suburb of Detroit, Michigan.

34. Based on my training and experience, and as described in paragraph 23, cybercrime actors often use residential proxy services to use an IP address that is geolocated nearby their victim to bypass fraud detection systems and appear to be legitimate.

35. On April 3, 2023, the Honorable Michael J. Roemer, U.S. Magistrate Judge of the United States District Court for the Western District of New York, signed a federal search warrant for DODGE and the PREMISES.

36. On April 4, 2023, the FBI executed the aforementioned search warrant at the PREMISES and seized multiple electronic devices and papers from the PREMISES. As relevant to this affidavit, agents found a written note in the PREMISES that appeared to list the username "cakesbaylor" for "911.re" and the username "napscickdinner@proton" for IPVanish. Based on my training and experience, I know that the 911.re proxy service was a residential proxy network that shutdown in 2022 and that IPVanish is a VPN service. As noted above, Genesis user cakesbaylor appeared to use residential proxy networks to use stolen credentials that he had purchased from Genesis Market. A photograph of the handwritten note is pictured below.



37. In the course of the search on April 4, 2023, FBI agents interviewed DODGE. DODGE told agents, among other things, that (1) he had learned about Genesis Market from an online advertisement and was invited to join Genesis Market by an unnamed individual while participating in a private online chat room; (2) he had purchased information from Genesis Market, that included user credentials (usernames and passwords) and internet cookie files that could make DODGE seem like the true owner of the credentials and; (3) that he made around 10 purchases from Genesis Market and estimated that he paid less than $100 for the stolen

credentials and; (4) he was never able to successfully log into accounts associated with the stolen credentials he purchased from Genesis Market.

CONCLUSION

38. Based on the foregoing, I respectfully submit that there is probable cause to believe that COREY ROBERT DODGE did violate of Title 18, United States Code, Section 1029(a)(3) (knowingly and with intent to defraud possessing fifteen or more devices which are counterfeit or unauthorized access devices). I respectfully request that the Court issue the attached criminal complaint, as well as an arrest warrant. To allow the warrant to be effectuated, I respectfully request that the criminal complaint, this affidavit, and the arrest warrant remain under seal.

Respectfully submitted,

Bryan Scheiber
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me, telephonically on April 27, 2023

HON. MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE